PEARSON, J.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	CASE NO. 5:18-CR-448
	)	
Plaintiff,	)	
	)	JUDGE BENITA Y. PEARSON
v.	)	
	)	
PHILIP M. POPA, JR.,	)	**MEMORANDUM OF OPINION AND**
	)	**ORDER** [Resolving ECF Nos. 22, 23, 24,
Defendant.	)	25]

There are four motions pending before the Court. Defendant moves for leave to file evidentiary motions *instanter* (ECF No. 22), to compel production of certain evidence (ECF No. 23), to suppress certain evidence (ECF No. 24), and to appoint Tami Loehrs as an expert for the defense (ECF No. 25). The first is granted; the latter three are denied.

I. Background

In April 2018, Federal Bureau of Investigation ("FBI") Agent Ryan Anschutz was operating undercover on an Internet-based, peer-to-peer network known as "Freenet." ECF No. 23-1 at PageID#: 96. Users of Freenet can share files anonymously and chat with one another on message boards. Agent Anschutz observed that a user with a given IP address had requested pieces of child pornography files. Using a complex algorithm (discussed below), Agent Anschutz concluded that the user of that IP address was the original requestor of those files. *Id.* at PageID#: 95-96.

On June 1, 2018, using a publicly available search tool, Agent Anschutz discovered that the given IP address was registered to Time Warner Cable. *Id.* at PageID#: 99. The FBI sent an administrative subpoena to Time Warner asking for rudimentary subscriber information about the user behind that IP address, including the person's name, address, phone number, email address, and other similar data. *Id.* Based on the information returned by Time Warner and the information discovered during his Freenet investigation, Agent Anschutz requested a warrant to search Defendant's residence and seize his HP laptop computer. ECF No. 23-1. In the affidavit supporting the search warrant, he described the methodology of his Freenet investigation, and he explained that the algorithm he used was supported by a publicly-available, peer-reviewed academic paper. *Id.*

A federal magistrate judge issued the requested warrant on July 17, 2018, and the warrant was executed the same day. ECF No. 1-1. During an interview with law enforcement, Defendant admitted to using Freenet to view and download child pornography on his HP laptop computer. *Id.* He described the content of a file he had downloaded, which matched the description of a file Agent Anschutz had observed in April. *Id.* Defendant was subsequently indicted on one count of Receipt of Visual Depictions of Real Minors Engaged in Sexually Explicit Conduct in violation of 18 U.S.C. § 2252(a)(2), and one count of Possession of Child Pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). ECF No. 11.

On January 29, 2019, defense counsel requested a copy of the academic paper relied on by Agent Anschutz in the affidavit supporting the search warrant as well as an installable copy of the software Agent Anschutz used in his Freenet investigation. ECF No. 26-4. The Government provided a copy of the academic paper, but it did not provide a copy of the software. *Id.* When the Government learned that defense counsel also wanted a copy of Agent Anschutz’s Freenet log files, the Government immediately produced them. ECF No. 26-5.

On February 11, 2019, six days after the cutoff to file pretrial motions, Defendant filed four motions: one for leave to file motions *instanter* (ECF No. 22), one to compel production of certain evidence (ECF No. 23), one to suppress certain evidence (ECF No. 24), and one to appoint an expert for Defendant (ECF No. 25). The latter three have been fully briefed (ECF Nos. 26, 27), and they are discussed below.

II. Law and Analysis

A. Motion to Compel Production (ECF No. 23)

Defendant moves the Court to compel production of all log files created by Agent Anschutz in his Freenet investigation on April 21, 2018, and an installable copy of the law enforcement software utilized in that Freenet investigation. ECF No. 23. The Government has already satisfied Defendant’s first request. ECF No. 26 at PageID#: 274. The remaining question is whether Defendant is entitled to inspect the secret software available only to sworn law enforcement officers the “Law Enforcement Freenet” software.

Pursuant to Fed. R. Crim. P. 16(a)(1)(E), a defendant is entitled

> to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions of any of these items, if the item is within the government’s possession, custody, or control and:
>
> (i) the item is material to preparing the defense;
> (ii) the government intends to use the item in its case-in-chief at trial; or
> (iii) the item was obtained from or belongs to the defendant.

Defendant argues for production of the software on the basis that the inner workings of the software are material to preparing his defense.[1] ECF No. 23 at PageID#: 75-79. The Government resists production, arguing that Defendant has not made a specific showing that the requested evidence is material to his defense. "To obtain discovery under Rule 16, a defendant must make a *prima facie* showing of materiality. Neither a general description of the information sought nor conclusory allegations of materiality suffice; a defendant must present facts which would tend to show that the Government is in possession of information helpful to the defense." *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990); *see* *United States v. Pirosko*, 787 F.3d 358, 367-68 (6th Cir. 2015). "Under Rule 16(a)(1)[(E)], a defendant may examine documents material to his defense, but, under Rule 16(a)(2), he may not examine Government work product in connection with his case." *United States v. Armstrong*, 517 U.S. 456, 463 (1996).

Defendant first argues that the inner workings of the Law Enforcement Freenet software might expose inaccuracies that would impeach Agent Anschutz's search-warrant affidavit. ECF No. 23 at PageID#: 75-76. Consequently, he argues, the later-discovered evidence would necessarily be suppressed. *Id.* This argument confuses the motions at bar. A motion to compel under Rule 16 is not a motion to suppress. At trial, the jury will not be asked to assess the legality of the FBI's search or the sufficiency of the evidence supporting the predicate search warrant. "[I]n the context of Rule 16 'the defendant's defense' means the defendant's response

[1] Defendant also asserts, in passing, that "the Freenet software is a critical component of the Government's case-in-chief." ECF No. 23 at PageID#: 76. He does not advance an argument, however, that the Court should compel production of the software on that ground.

to the Government's case in chief," not pretrial motions. *Armstrong*, 517 U.S. at 463; *see United States v. Arambula*, 82 F. Supp. 3d 1316, 1319 (D.N.M. 2014) ("'[P]reparing the defense' in this context deals exclusively with rebuttal of the government's case-in-chief, not the preparation of affirmative defenses, much less challenging the sufficiency of the evidence that supported a warrant."). Defendant's first argument fails.

Second, Defendant relies on a Ninth Circuit case in which the court ruled that a similar peer-to-peer file-sharing software had to be produced because it was material to preparing the defense. *United States v. Budziak*, 697 F.3d 1105 (9th Cir. 2012). *Budziak* is factually distinct from this case. In *Budziak*, the defendant was charged with knowingly distributing child pornography files. *Id.* at 1112. To prove its case, the government had to show that the defendant not only possessed child pornography files on his computer or had received them from someone else, but that he shared complete files with others and was aware that he had shared them with others. *Id.* To make that case, the government demonstrated that the files on the defendant's computer were complete, that he maintained those files in a shared folder, and that he knew that his shared-folder setting made those files available for downloading by others. *Id.* at 1109.

The government's software in that case was directly material to both the government's case in chief and the defendant's defense. Had the defendant been familiar with the government's software when he went to trial, he could have put the government to its proof on specific elements of the alleged offense. Why, for example, should the jurors believe that the files were complete, rather than fragmentary, when they were transmitted by the defendant to the agents? Or, how could the jurors be sure that the agents had not manipulated his shared-folder settings themselves? Either such inquiry might have raised a reasonable doubt as to a specific element of the offense with which the defendant was charged, and both inquiries were unavailable to the defendant for lack of familiarity with the government's evidence-gathering mechanism.

In this case, Defendant is not accused of distribution. ECF No. 11. Instead, he is accused of (1) receipt of visual depictions of real minors engaged in sexually explicit conduct, and (2) possession of child pornography. *Id.* *Budziak*'s potential lines of inquiry are not relevant to Defendant's case. Defendant makes no real suggestion that the Government will rely on evidence derived directly from the software, nor that it will try to persuade the jury of the software's accuracy and reliability. Rather, the Government seems likely to present evidence gathered from its July 17, 2018, search of Defendant's residence, the seizure of his computer, and the statement he made to the FBI agents at that time. *See* ECF No. 26 at PageID#: 264.

Defendant is not entitled to production of the Law Enforcement Freenet software because he cannot show that such production is material to preparing his defense. The motion to compel (ECF No. 23) is denied.

B. Motion to Suppress (ECF No. 24)

Defendant moves the Court to suppress all evidence derived from (1) the administrative subpoena issued to Time Warner, and (2) the subsequent warrant used to search Defendant's house and seize his computer. ECF No. 24.

1. Third-Party Doctrine

Defendant asks the Court to suppress all evidence resulting from the Government's administrative subpoena of Time Warner, arguing that the subpoena was itself a search that required a warrant under the Fourth Amendment. ECF No. 24 at PageID#: 155-58. Defendant acknowledges that Fourth-Amendment jurisprudence has long excluded from protection information voluntarily shared with a third party. *Id.* at PageID#: 156. He further acknowledges that he voluntarily conveyed his subscriber information to Time Warner when he contracted to receive internet service. *Id.* Citing *Carpenter v. United States*, 138 S. Ct. 2206 (2018) and two recent Supreme Court dissents, Defendant argues that the third-party doctrine either has been or should be altogether overruled.

The Supreme Court in *Carpenter* did not purport to upend or overrule the third-party doctrine. Rather, it acknowledged that "individuals have a reasonable expectation of privacy in the whole of their physical movements," even when those movements are passively disclosed to a cell-phone service provider through a global positioning system. *Carpenter*, 138 S. Ct. at 2216-17. The Court expressly did not overrule the third-party doctrine; rather, it "decline[d] to extend" it "to cover these novel circumstances." *Id.* at 2217.

Defendant voluntarily disclosed his subscriber information to Time Warner when he contracted to receive internet service. In doing so, he surrendered his privacy interest in that information. The FBI was not required to obtain a warrant before insisting that Time Warner disclose that information. The motion to suppress (ECF No. 24) is denied as to this ground.

2. *Franks v. Delaware*

Defendant argues that the warrant used to search his house and seize his computer "rel[ied] upon statements in an affidavit that [were] knowingly false or exhibit[ed] a reckless disregard for truth." ECF No. 24 at PageID#: 159. In keeping with *Franks v. Delaware*, 438 U.S. 154 (1978), he states, he is entitled to an evidentiary hearing on the matter because he has made a "substantial preliminary showing" that Agent Anschutz (the affiant) knowingly or recklessly made a false statement on his affidavit, and that false statement was necessary to the finding of probable cause that supported the search warrant. *See Franks*, 438 U.S. at 155-56.

In a thorough affidavit, Agent Anschutz explained the mathematical formula that he had employed to identify Defendant as the anonymous internet user who requested a file containing child pornography. ECF No. 24-1. Because the peer-to-peer sharing platform (Freenet) is complex and anonymized by design, that formula was necessarily complex. In requesting a warrant, Agent Anschutz assured the magistrate judge that the complex formula he used was published in an openly-available, peer-reviewed academic paper. *See* ECF No. 24 at PageID#: 157-59. Defendant asserts that the paper is not peer-reviewed, that Agent Anschutz knew it was not peer-reviewed at the time he swore the affidavit, and that the fact of peer review was necessary to the magistrate judge's finding of probable cause. *Id.*

Defendant is incorrect. The Government has shared the paper in question with Defendant and the Court. ECF No. 26-1; *see* ECF No. 26-4. It is titled *Statistical Detection of Downloaders in Freenet*, and it is written by researchers at the University of Massachusetts, Amherst, and the Rochester Institute of Technology in New York. ECF No. 26-1 at PageID#: 300. At the bottom of the first page, the paper contains a 2017 Copyright notation and a reference to the IEEE International Workshop on Privacy Engineering in May 2017 that reviewed the paper. *Id.* The Government has since provided additional information about that peer review. ECF No. 26-2 at PageID#: 308 ("Reviews has (sic) been done in accordance with IEEE guidelines . . . .").

Agent Anschutz did not make a false statement when he attested that the academic paper he relied on in performing his investigation was peer-reviewed. Defendant's suggestion to the contrary is without merit. The motion to suppress (ECF No. 24) is denied as to this ground.

C. Motion to Appoint Expert (ECF No. 25)

The denial of the first two motions (ECF Nos. 23, 24) renders moot Defendant's motion to appoint a defense expert (ECF No. 25). Defendant's proposed expert, Tami Loehrs, is experienced in computer forensics. ECF No. 25. In an affidavit, Ms. Loehrs describes the kind of assistance she hopes to offer Defendant if she is appointed an expert in this matter. ECF No. 25-1. The entirety of that affidavit pertains to the potential usefulness of inspecting the Government's Freenet software and the purported insufficiency of the evidence underlying the search warrant. Because Defendant's corresponding motions have been denied, the motion to appoint an expert (ECF No. 25) is also denied.

III. Conclusion

For the reasons provided, Defendant's motion for leave to file *instanter* (ECF No. 22) is granted. His motion to compel production (ECF No. 23), his motion to suppress evidence (ECF No. 24), and his motion to appoint an expert (ECF No. 25) are denied. These motions are readily resolved without a hearing. The hearing scheduled for March 1, 2019, at 11:00 a.m., is cancelled.

In place of a hearing, on March 1, 2019, at 11:00 a.m., the Court will hold a telephonic conference to address scheduling matters. Only counsel need attend. Assistant United States Attorney Carol M. Skutnik shall set up the conference call by joining defense counsel and calling the Court at (330) 884-7435.

Trial will begin on March 4, 2019, at 9:00 a.m.

IT IS SO ORDERED.

February 27, 2019
Date

/s/ Benita Y. Pearson
Benita Y. Pearson
United States District Judge